METHOD AND SYSTEM FOR PROVIDING DATA SECURITY USING FILE SPOOFING

This application is a U.S. national stage application of PCT International Application No. PCT/US00/26858 filed Sept 29, 2000 which claims priority to provisional application 60/157472 filed Oct 1, 1999 and provisional application 60/206947 filed May 25, 2000.

Field of the Invention

The present invention pertains to the field of file systems in electronic computers. In particular, the invention relates to a method and system for providing data security using file spoofing.

Background of the Invention

Data security is a serious concern of computer users and owners of intellectual property. It is increasingly common to use measures such as encryption to secure data files, to protect data from loss or unauthorized activity.

Computer systems typically include one or more local or networked data storage devices. A typical application program executing on such a computer system accesses such data storage devices by calling standard file system services provided by an operating system, such as services for creating, reading, and writing files on the data storage devices.

A device driver is a set of computer-implemented instructions that implements the device-specific aspects of generic input/output operations. In typical operating systems, software applications such as device drivers run in either "kernel mode" or "user mode." A virtual device driver is a type of device driver that has direct access to an operating system kernel, such as by running in kernel mode. "Kernel mode" is a highly privileged memory access mode of the processor. "User mode" is a less privileged memory access mode of the processor. The memory access mode is a part of the hardware state of the processor. The kernel mode privilege level is also known as "Ring 0," and the user mode privilege level is also known as "Ring 3." Kernel mode access allows the virtual device driver to interact with system and hardware resources at a very low level.

In conventional operating systems, device drivers may be represented as layered on top of one another. The layered architecture is also sometimes referred to as a stack or a calling chain. It is the lowest-level device driver that typically controls a hardware device. If there is only a single device driver above the hardware device, the driver is called a monolithic driver. However, a plurality of drivers may be placed above the lowest-level driver. Input and output requests ("I/O requests") to the hardware device or devices controlled by a lowest-level driver are handled first by the highest-level driver, then seriatim by any lower-level intermediate drivers,